

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

_____X

OUSSAMA EL OMARI,

Plaintiff,

Case No.: 23-cv-____ () ()

v.

COMPLAINT

DECHERT LLP,
NICHOLAS PAUL DEL ROSSO, and
VITAL MANAGEMENT SERVICES, INC..

Defendants.

_____X

OUSSAMA EL OMARI, Plaintiff in the above referenced action, by and through his undersigned counsel, MOORE INTERNATIONAL LAW PLLC, as and for his Complaint, states as follows:

INTRODUCTION

1) This case involves evidence discovered in January 2023 by Plaintiff Oussama El Omari, that Defendant Nicholas Del Rosso, a private investigator employed by El Omari's adversary in prior litigation, Defendant Dechert LLP, illegally obtained and possessed a tranche of confidential and privileged attorney-client email communications between El Omari and his undersigned counsel. The Defendants did so by engaging Indian hackers to hack into El Omari's email account in 2017 and copied his legal email correspondence. El Omari seeks equitable and injunctive relief, and compensatory and punitive damages to deter Defendants and their co-conspirators from engaging in similar illegal and unethical conduct. Until he was informed in January 2023 that a copy of his attorney's emails was discovered on Del Rosso's Laptop, El Omari was unaware that his email account was hacked. El Omari's causes of action here accrued

in January 2023 when he discovered his injury. There is other similar litigation against the Defendants in the U.S. and U.K. by at least five other Dechert LLP adversaries with allegations similar to this case.

2) The illegal “surveillance-for-hire” described in this case involves three stages: “reconnaissance,” “engagement,” and “exploitation.” The third stage, “exploitation,” is known as “hacking for hire.” For a detailed description, see Facebook’s parent, Meta’s *2021 Threat Report on the Surveillance-for-Hire Industry*. Here, the illegal hack for hire intelligence gathering was deployed by sending El Omari phishing emails intended to trick him and steal his email account login credentials, and using the stolen credentials to illegally access, copy, and store his attorney-client communications for use against him in adversarial proceedings in this District.

THE PARTIES

3) Plaintiff Oussama El Omari (“El Omari”) is a U.S. citizen residing in Raleigh, North Carolina. El Omari was the plaintiff in the previous New York litigation (the “NY litigation”) described below.

4) Defendant Dechert LLP is a limited liability partnership law firm headquartered in Philadelphia, Pennsylvania, with offices in New York, London, Dubai, and other locations. In the previous New York litigation, Dechert LLP’s New York office (“Dechert NY”) and its attorney, Linda Goldstein (“Goldstein”) were adverse in actual litigation with El Omari since May 2016. In the prior adversarial proceedings in this District, Dechert NY represented its clients, prior defendant Sheikh Saud Bin Saqr Al Qasimi, (“Saud” or “the Ruler”), the Ruler of Ras al Khaimah, (“RAK”), an Emirate of the United Arab Emirates, (“UAE”), and prior defendant the Ras Al Khaimah Free Trade Zone Authority, (“RAKFTZA”), a governmental entity under his authority.

5) Defendant Nicholas Paul Del Rosso (“Del Rosso”) resides in Chapel Hill, North Carolina. Del Rosso is a private investigator. Del Rosso is the owner and president of his closely held Vital Management Services, Inc. Del Rosso directs the affairs of Vital. Del Rosso has been a private investigator for Dechert LLP since approximately August 2014 when he was hired by David Neil Gerrard, (“Gerrard”), an attorney at Dechert LLP’s office in London, United Kingdom, (“Dechert London”), in relation to Dechert LLP’s representation of the Ruler and RAK governmental entities under his authority. Del Rosso’s working relationship with lawyers at Dechert LLP began approximately one to four years prior to 2014 when Del Rosso worked with an attorney named Abousleiman and his staff at a prior law firm before joining Dechert LLP.

6) Defendant Vital Management Services, Inc. (“Vital”) is a corporation organized under the laws of North Carolina which provides private investigative services. Vital’s office is located at Del Rosso’s place of residence in Chapel Hill, North Carolina.

THE NON-PARTY CO-CONSPIRATORS

7) CyberRoot Risk Advisory Private Limited (“CyberRoot”) is a name known in the mercenary cyber hacking industry. CyberRoot is a firm with its office located in Gurgaon, India. In 2022, CyberRoot was the focus of Meta’s *2022 Threat Report on the Surveillance-for-Hire Industry*, in which Meta reported removal of a network of over 40 Facebook and Instagram accounts used by CyberRoot for its hacking activities related to, among other methods, phishing activities intended to trick targets into giving up their email credentials.

8) David Neil Gerrard is an attorney who at all relevant times was employed by Dechert LLP at its London office in the United Kingdom. Gerrard worked closely with Dechert

NY and its attorney, Linda Goldstein, relative to their common clients, the Ruler, and RAK governmental entities under his authority.

9) Linda Goldstein is an attorney who at all relevant times was employed by Dechert NY. Goldstein and Dechert NY were adverse to El Omari in his previous New York litigation.

10) Aditya Jain (“Jain”) is a resident of India. Upon information and belief, at all relevant times, Jain was a go-to-ringleader of an unincorporated association of Indian hackers named WhiteInt run by Jain in Gurugram, India. The participants in the hacking ring included Jain, CyberRoot, another Indian hack-for-hire firm named BellTrox, and others, which commonly shared hacking equipment and staff. Jain held a full-time job as an associate director of Deloitte India’s cyber security unit until his hacking exploits were publicized and he was fired in November 2022.

11) Sheikh Saud Bin Saqr Al Qasimi is the Ruler of Ras Al Khaimah. At all relevant times, the Ruler and RAKFTZA were clients of Dechert NY. El Omari previously worked in RAK for Saud’s brother and political rival, Sheikh Faisal Bin Saqr Al Qasimi (“Faisal”) until El Omari was wrongfully terminated by Saud in 2012 during a political power struggle between Saud and Faisal. El Omari was subsequently wrongfully persecuted by Saud, which figured in El Omari’s prior NY litigation.

JURISDICTION AND VENUE

12) This Court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1331 (federal question jurisdiction). Jurisdiction over state law claims is based on 28 U.S.C. § 1367 (supplemental jurisdiction).

13) Jurisdiction is proper over Dechert LLP because Dechert NY is in New York county. Dechert NY was defense counsel of record in El Omari’s prior NY litigation in this

District. The purpose of the alleged hacking of El Omari's confidential and privileged legal communications was to provide illegal intelligence about El Omari's knowledge and information about the Ruler, legal positions, strategies, witnesses, evidence, and funding to assist Dechert NY in the adversarial NY litigation.

14) Jurisdiction is proper over Del Rosso because as Dechert LLP's private investigator, he is an agent of Dechert LLP. Del Rosso directed the hacking of El Omari through CyberRoot, the hacking agent in India, and reported the resulting illegal intelligence for use against El Omari in this District. Upon information and belief, Del Rosso made numerous trips to New York for personal meetings as part of his wrongful activities.

15) Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) and 18 U.S.C. §§ 1965(a) and (b), because a substantial part of the events giving rise to the claim occurred in this District, including Dechert NY and Goldstein receiving and using the illegal intelligence gained from El Omari's hacking to advance their litigation defense in this District.

STATEMENT OF FACTS

The Prior New York Litigation

16) The undersigned attorney and law firm have been counsel for El Omari since April 11, 2016 to the present, and have brought cases on El Omari's behalf for various claims arising out of his past employment as Director of RAKFTZA.

17) In Case No. 16-cv-3895 in this District, El Omari brought a complaint on May 25, 2016 against RAKFTZA and Kreab (USA) Inc. Defendants Saud and The Arkin Group LLC were added by later amendment. The causes of action advanced by El Omari alleged Breach of Contract, Fraud, and Intentional Infliction of Emotional Distress, relating to, among other things, an alleged false smear report involving Iranian sanction violations occurring in RAKFTZA, of

which El Omari was Chairman, prepared as a pretext for his unjustified firing in 2012 by Saud and his subsequent communications to U.S. Customs seeking El Omari's arrest. This case brought by El Omari was subsequently dismissed in 2017 at the pleading stage on the basis of foreign official immunity (Saud) and failure to state a claim (remaining defendants), and was upheld on appeal on August 23, 2018. Dechert LLP, by Linda Goldstein, was defense counsel for defendants Saud and RAKFTZA.

18) In Case No. 20-cv-2601 also brought in this District, a complaint was filed on March 27, 2020 by El Omari against James Buchanan, Dechert LLP, Andrew Frank, Neil Gerrard, Amir Ali Handjani, Karv Communications Inc., Intelligence Online, and Longview Partners (Guernsey) Limited. The complaint alleged Civil Racketeer Influenced and Corrupt Organizations ("RICO") Act violations by Karv, Frank, and Handjani, and *Prima Facie* Tort, Defamation, and violation of the Computer Fraud and Abuse Act against all defendants. In those proceedings, El Omari, among other things, alleged the existence of a continuing and organized false smear campaign against him, including a plant of false facts in a publication by Dechert LLP and Gerrard that El Omari was falsely involved in a billion-dollar fraud scheme involving his alleged employer, RAKIA, an entity under Saud's authority that El Omari never worked for. That campaign was alleged to have also involved fake emails sent to El Omari to trick him into granting interviews to a fake Fox News NY journalist who posed questions relating to Faisal, other perceived enemies of Saud, and about El Omari's own litigation pending at that time. This case was subsequently dismissed at the pleading stage in 2021 for failure to state a claim, and was upheld on appeal on October 18, 2022. Dechert LLP defended itself and Gerrard. Goldstein was an attorney of record.

The January 2023 Discovery of Hacked Legal Correspondence on the Laptop of Dechert LLP's Investigator Del Rosso

19) On January 13, 2023, just months after the last case in the NY litigation was upheld on appeal, El Omari's undersigned counsel received a foreign notice pursuant to a U.K. court order, concerning disclosure in London of the discovery of three data storage devices. ("the U.K. notice"). The U.K. notice was pursuant to other, but similar, hacking litigation currently pending in London against Dechert LLP, Gerrard, and other Dechert attorneys.¹ ("the U.K. litigation"). One device, a laptop, was found to contain a backup copy of emails containing the email address of El Omari's undersigned counsel (smm@milopc.com). This disclosure did not include the email contents or identify any sender or recipient addresses. The evidence shows to be communications between El Omari and his undersigned attorney. This Laptop disclosure was previously unknown and a surprise to El Omari and his undersigned counsel. The disclosed date range of data found on the laptop was before and during representation of El Omari and the NY litigation. The three drives have been claimed by adversaries from the NY litigation. Del Rosso's involvement as Dechert LLP's private investigator in El Omari's prior NY litigation was previously unknown. At present, the three devices are in the possession of Stokoe Partnership Solicitors, ("Stokoe"), the plaintiff attorneys in the U.K. litigation. El Omari's former adversaries, Del Rosso, Dechert LLP, and Buchanan claim ownership of the devices and are currently litigating in the U.K. litigation to regain possession of the devices from Stokoe.

¹ Consolidated cases of *Al Sadeq v. Dechert LLP, Neil Gerrard, David Hughes, and Caroline Black*, Claim No. QB-2020-000322, *Stokoe Partnership Solicitors v. Dechert LLP David Neil Gerrard*, Claim No. QB-2020-002492, *Quzmar v. Dechert LLP and Neil Gerrard*, Claim No. QB-2020-003142, In the High Court of Justice, King's Bench Division.

20) The U.K. notice disclosed that a Huawei Matebook laptop, manufactured in 2019, with identification, “S/N: EHUBB18C10000878,” and labelled “P-SH,” (“the Laptop”), contained emails from five email accounts relating to Del Rosso, (ndr99@email.com, ndr100@usa.com, ndr@vitalmanage.com, ndr100@usa.com), and his son, Leo Del Rosso, (leo@acceptances.co.uk), as well as an unauthorized backup tranche of emails containing the undersigned’s professional email address, (smm@milopc.com). Del Rosso asserted a claim of ownership of the Laptop in the U.K. litigation. Del Rosso has admitted to being a private investigator employed by Dechert LLP since approximately August 2014. Dechert LLP is the same law firm, adverse to El Omari and the undersigned counsel in the NY litigation. The file on the Laptop containing El Omari’s undersigned counsel’s email address was found to be part of a file called “update24Jan.rar.” This filename containing the word “update” suggests the email tranche on the Laptop itself builds on previous intelligence reports. The data on the Laptop, determined to be between March 2011 and May 2021, is during the period leading up to El Omari’s RAKFTZA employment termination in 2012 and subsequent NY litigation from 2016 onward. The Laptop was determined to have been manufactured in 2019. El Omari’s subsequent investigation determined the hacking of an email account of El Omari occurred on or about January 12, 2017, as described below. The timing of the Laptop manufacturing date which predates the emails contained thereon indicates that the illegal email tranche in “update24Jan.rar” on the Laptop was copied from another source in 2019 or later and is itself a copy.

21) The other two other devices besides the Laptop are an Aegis portable drive, with product identification, “Padlock 3 A25-3PL256-1000,” and labeled “Client,” (the “Aegis Device”), which is password protected, and a Seagate portable drive, with product identification,

“S/N: NAASFRFT,” and labeled, “USB & JB MBA,” (the “Seagate Device”). Del Rosso and Dechert LLP both claim ownership of the Aegis Device in the U.K. litigation. The Seagate Device was found to contain two email addresses relating to James Buchanan, also a prior defendant in the NY litigation. Buchanan has claimed ownership of the Seagate Device in the UK litigation. Collectively, the Laptop, the Aegis Device, and the Seagate Device are referred to here as “the Devices.”

El Omari’s Subsequent Hacking Investigation

22) The January 2023 disclosure of the Laptop and its unlawfully obtained email contents triggered an investigation to determine what email account was hacked to obtain the stolen email tranche found on the Laptop. El Omari’s undersigned counsel found no evidence the email account, smm@milopc.com, was hacked. El Omari’s investigation showed one of El Omari’s email accounts, ceo@oussamaelomari.com, was hacked on or about January 12, 2017. The stolen email tranche thus was copied from El Omari’s hacked email account (“ceo@oussamaelomari.com”).

23) This investigation found El Omari received related three phishing emails in December 2016 and January 2017 sent to two of his email addresses, ceo@oussamaelomari.com and abousami2793@gmail.com. This timing is shortly after El Omari’s first case in the NY litigation was filed in this District in May 2016.

24) The first phishing email was sent by an “Amad Nimeh” (amad.nimeh@presidency.com) on December 20, 2016, to El Omari’s Gmail email address (abousami2793@gmail.com). El Omari did not respond to this email.

25) The second phishing email was sent by a “Matt Rosen” (matt.rozen@ctfcomms.co) on January 3, 2017 to El Omari’s Microsoft Outlook email address,

ceo@oussamaelomari.com. This email was a purported speaking invitation by a purported conference organizer for the “Adobe Summit EMEA 2017,” which was similar to MELA, an organizer which presented El Omari with an award for best free zone manager in 2006. This email showed research into El Omari’s professional associations, and was designed to gain the trust of and engage El Omari. In truth, these two emails, December 20, 2016 and January 3, 2017, actually came from the same email address, “email81.com.”

26) When El Omari responded, thinking the email was genuine, and declined the speaking engagement by a reply email on January 10, 2017, “Matt Rosen” followed up with another email two days later on January 12, 2017, sent to El Omari’s Microsoft Outlook email address, ceo@oussamaelomari.com, and copied to his other address, abousami2793@gmail.com. This email by “Matt Rosen” was an attempt to overcome El Omari’s declining the invitation by attempting to persuade El Omari to speak remotely by video. This email contained an attachment which El Omari was asked to open to see videos and other information about past conferences. Forensic examination of this email of January 12, 2017 sent to El Omari’s Microsoft Outlook email address, ceo@oussamaelomari.com, determined it actually came from “web-hosting.com,” not “email81.com” like “Matt Rosen’s” earlier email of January 10, to further obfuscate the email source.

27) In truth, Matt Rosen was an impostor, and his visible email address, matt.rozen@ctfcomms.co, was designed to imitate a legitimate website of a public relations company, “ctfcomms.com.” This January 12 email actually contained a malicious attachment. When opened, the document contained three links to purported videos from previous speakers and other information. In truth, two of the links, the first and third (top to bottom), were illegitimate and went to a website named “internetsecuritystandards.site,” rigged to steal El

Omari's email login and password credentials. El Omari unwittingly clicked on the first link and saw a page of computer language he did not understand. It is consistent with such a malicious website that when El Omari clicked on this first link, malware with the capability to steal his login credentials was automatically downloaded onto El Omari's computer. The password stealing website, "internetsecuritystandards.site," was not visible to the viewer in the first and third attachment links. This malicious password stealing website was created on the same day this email was created, January 12, 2017, and the website was deleted a month later on February 19, 2017, indicating a successful email credential steal and hack of El Omari's Microsoft Outlook email account ceo@oussamaelomari.com.

28) On or about January 12, 2017, but no later than February 19, 2017, the lifespan of the password stealing website, "internetsecuritystandards.site," El Omari's Microsoft Outlook email account, ceo@oussamaelomari.com, was accessed without his authorization using his stolen login credentials. This occurred by the hacker logging into El Omari's online Microsoft Outlook email account, ceo@oussamaelomari.com, which uses a Microsoft data center, a physical location containing physical computer devices for the processing and storing of data.

29) It is consistent with such deployment that the hacker also accessed, monitored, and copied from this email account of El Omari for information after this time period with the stolen login credentials.

30) Confidential and privileged email communications between El Omari and his undersigned attorney were copied from El Omari's email account and disseminated for use against him in the NY litigation. Since Del Rosso's Laptop copy appears to be itself a copy and part of an "update," it is presently unknown how many other copies of the illegal email tranche may exist and who possesses them. These law emails would contain confidential information,

such as El Omari's legal strategy, witnesses, evidence, and funding about the NY litigation defended by Dechert LLC.

31) The three emails sent to El Omari are summarized as follows.

Date	Account Type	Account Holder
12/20/2016	Gmail Email Account, abousami2793@gmail.com	Oussama El Omari
01/03/2017	Microsoft Outlook Email Account, ceo@oussamaelomari.com	Oussama El Omari
01/12/2017	Gmail and Microsoft Outlook Email Accounts, ceo@oussamaelomari.com abousami2793@gmail.com	Oussama El Omari

The above phishing emails were sent to and received by El Omari at his two computers (one laptop and one desktop) at his home in Raleigh, North Carolina. El Omari opened emails to his address, abousami2793@gmail.com, on his laptop computer. El Omari opened emails to his address, ceo@oussamaelomari.com, on his desktop computer.

The More Than \$500,000 in Hacking Payments by Dechert LLP's Private Investigator Del Rosso

32) Del Rosso paid Indian hackers to hack into the email communications of El Omari, and others, by using Vital's bank account to pay CyberRoot for hacking.

33) Del Rosso sent dozens of international wire transfers from Vital's bank in North Carolina to CyberRoot's bank in Haryana, India, totaling more than \$500,000 just between 07/28/2015 and 12/23/2016. Del Rosso's hacking instructions and related communications with

CyberRoot, upon information and belief, were in part through Jain, the Indian hacking ringleader. Upon information and belief, Jain's hacking database contains both of El Omari's email addresses. Jain's database is believed to also show that Del Rosso gave Jain over 40 hacking target names.

34) Wire transfers from Del Rosso to CyberRoot during this period are as follows.

Date	Amount (USD)	Sender	Receiver
07/28/2015	5,459	Vital, NC	CyberRoot, Haryana, India
03/14/2016	7,500	Vital, NC	CyberRoot, Haryana, India
03/15/2016	7,500	Vital, NC	CyberRoot, Haryana, India
05/10//2016	10,000	Vital, NC	CyberRoot, Haryana, India
05/16//2016	14,991.67	Vital, NC	CyberRoot, Haryana, India
05/20//2016	42,491.67	Vital, NC	CyberRoot, Haryana, India
06/07/2016	47,991.67	Vital, NC	CyberRoot, Haryana, India
06/10//2016	7,500	Vital, NC	CyberRoot, Haryana, India
06/16//2016	9,500	Vital, NC	CyberRoot, Haryana, India
07/19//2016	82,991.67	Vital, NC	CyberRoot, Haryana, India
08/03//2016	49,481.67	Vital, NC	CyberRoot, Haryana, India
08/26//2016	14,991.67	Vital, NC	CyberRoot, Haryana, India
09/06//2016	56,491.67	Vital, NC	CyberRoot, Haryana, India
09/12//2016	7,500	Vital, NC	CyberRoot, Haryana, India
09/16/2016	2,500	Vital, NC	CyberRoot, Haryana, India
09/27/2016	10,000	Vital, NC	CyberRoot, Haryana, India
10/10//2016	2,500	Vital, NC	CyberRoot, Haryana, India

10/13//2016	27,491.67	Vital, NC	CyberRoot, Haryana, India
10/18//2016	77,191.67	Vital, NC	CyberRoot, Haryana, India
10/27/2016	24,991.67	Vital, NC	CyberRoot, Haryana, India
11/04//2016	1,500	Vital, NC	CyberRoot, Haryana, India
11/10//2016	5,000	Vital, NC	CyberRoot, Haryana, India
11/15/2016	5,000	Vital, NC	CyberRoot, Haryana, India
12/07/2016	21,491.67	Vital, NC	CyberRoot, Haryana, India
12/22/2016	7,500	Vital, NC	CyberRoot, Haryana, India
12/23/2016	27,491.67	Vital, NC	CyberRoot, Haryana, India
Total: <u>\$577,049.04</u>			

35) Upon information and belief, Del Rosso paid further and other substantial payments to CyberRoot, Jain, and BellTrox, before and after the above period, and Del Rosso after the fact urged CyberRoot to prepare false invoices in an attempt to cover-up the true purpose of his hacking payments.

The Defendants Conducted Their Affairs as a Conspiracy.

36) The purpose of the conspiracy was to hack and access confidential emails of El Omari, and other Dechert LLP's litigation adversaries. The relationships consisted of Dechert LLP, its lawyers Gerrard and Goldstein, their private investigator Del Rosso, Del Rosso's company Vital, CyberRoot, Jain, and possibly the participation of others. The longevity of the conspiracy began at the latest in July 2015 when Del Rosso started paying CyberRoot in wire transfers, and ended at the earliest in January or February 2017 when El Omari's email login credentials were stolen and his email account accessed and copied, and the malicious credential stealing website, "internetsecuritystandards.site," was deleted. It is likely the conspiracy started

earlier, and continued later in time, due to the fact that the data on Del Rosso's Laptop ranged from March 2011 to May 2021, which is during the period leading up to El Omari's employment termination at RAKFTZA in 2012, his prior U.A.E. litigation, and his subsequent NY litigation. The longevity, at its minimum period of 19 months, permitted the conspirators to pursue the conspiracy purpose of hacking El Omari's email account to obtain his confidential emails.

Dechert LLP and its Investigator Del Rosso Are Willful and Knowingly Culpable Persons

37) Del Rosso had actual knowledge of the illegal activities. The fact that Del Rosso's Laptop contains confidential attorney – client emails of an adversary of his client, Dechert LLP, shows Del Rosso's actual knowledge of illegal hacking by CyberRoot, a known mercenary hacker, which he hired and paid a substantial amount of money.

38) Dechert LLP either had actual knowledge, or must have strongly suspected the illegal hacking activities of its private investigator Del Rosso and CyberRoot. The substantial costs of over a half-million dollars paid to CyberRoot by Del Rosso, were in turn costs to Dechert LLP. The subsequent sharing of the sensitive information gleaned from the stolen confidential emails with Goldstein at Dechert NY must have triggered strong suspicions by Goldstein, an experienced and learned law professional, that El Omari's sensitive litigation information was illegally obtained. Since the information was found in emails between El Omari and his attorney, the emails and contents must have been strongly suspected as gained by illegal email hacking. Goldstein, trained in the law, and duty bound to comply with her own lawyer-client confidentiality obligations under the NYSBA Rules of Professional Conduct, including Rule 1.6 (Confidentiality of Information), must have deliberately avoided learning about the illegal sourcing of the sensitive information.

The Defendants' Acts Affected Interstate and Foreign Commerce

39) The acts of the Defendants affected interstate and foreign commerce due to the fact that El Omari, Del Rosso, and Vital are located in North Carolina, Del Rosso was hired by Gerrard at Dechert London and was paid by Dechert LLP, and the contents of El Omari's email law correspondence was used by Dechert New York. CyberRoot was paid by Del Rosso through Vital by numerous wire transfers from North Carolina to India. In addition, communication lines for electronic transmission of El Omari's confidential hacked emails, and information from them, are alleged to be between Del Rosso in North Carolina, Goldstein in New York, Gerrard in London, and CyberRoot in India.

The Defendants' Acts Proximately Caused Injury to El Omari

40) It is manifestly unfair to El Omari that he litigated against the Defendants in the NY litigation all the while Defendants were in possession of his privileged and confidential emails with his attorney.

41) The Laptop of Dechert LLP's investigator, Del Rosso, discovered in January 2023, has caused new and ongoing injury to El Omari beginning in January 2023. To date, El Omari's damages are in excess of tens of thousands of dollars paid to date in legal fees and costs, and forensic computer investigation costs related to investigating, assessing the scope of the hacking, and seeking to remedy the complete loss of the confidentiality of the emails.

42) El Omari sustained injuries to his business and property by reason of the Defendants' actions. The damage to El Omari, proximately caused by the violations, were pecuniary injuries to a proprietary interest. But for the Defendants' violations involving the hacking of El Omari's email account, El Omari would not have had to suffer monetary expenses of investigating the hacking and spending attorney fees and costs seeking to stop the use,

dissemination of, and to restore the confidentiality of the emails on the Laptop from the Defendants.

43) El Omari has suffered the complete loss of valuable confidentiality of the data in the attorney–client communication emails pertaining to El Omari’s NY litigation. This illegally obtained intelligence would include confidential information about matters and decisions related to investigations, witnesses, legal strategy, evidence, and funding, all of which El Omari takes an active and involved interest. The information had value not only because of the cost of legal services to El Omari at the time, but because of the role of the emails and information therein in the operation and decision-making in El Omari’s litigation.

44) Punitive damages are warranted because of the wanton, reckless, malicious, and oppressive character of the acts complained of. The Defendants hired and paid CyberRoot, a known mercenary cyber hacker, to gain sensitive and confidential intelligence about their adversary, El Omari. The hacking cost of \$577,049.04 in dozens of small wire transfer amounts during the time period is substantial for a private investigator. The specialized knowledge and duties imposed upon the Defendants by the NYSBA Rules of Professional Conduct, including Rule 1.6 (Confidentiality of Information), shows knowledge of their wrongful conduct and an intention to cover up and hide the defendants’ willful, reckless, and wanton disregard for the confidentiality rights of their hacking target, El Omari.

Statute of Limitations

45) Until El Omari was informed by the U.K. Notice on January 13, 2023 that a tranche of El Omari’s attorney’s emails were discovered on a Laptop in London, El Omari was unaware that any of his email accounts had been hacked. El Omari’s causes of action thus accrued on January 13, 2023 when thus alerted and discovering his injury.

46) El Omari reserves the right to amend his pleadings over the course of this lawsuit.

FIRST CAUSE OF ACTION

(18 U.S.C. § 1030(a)(2)(C) – Accessing a Protected Computer and Obtaining Information)

47) The factual allegations in paragraphs 16 through 46 are realleged and incorporated as if fully set forth herein.

48) On or about the date set forth below,

Dechert LLP, and
Nicholas Del Rosso,

by and through their agent, CyberRoot, did intentionally access a protected computer, a Microsoft Outlook email account of Oussama El Omari, without authorization, and did thereby obtain information from a protected computer.

Date	Account Type	Account Holder
01/12/2017	Microsoft Outlook Email Account, ceo@oussamaelomari.com	Oussama El Omari

49) The means of access without authorization was by CyberRoot sending phishing emails to El Omari, one of which sent on the above date tricked El Omari into going to a malicious password stealing website which worked to steal his email login credentials. CyberRoot, posed as fictional Matt Rosen with email address, matt.rozen@ctfcomms.co, and sent the malicious attachment. When El Omari opened the document and clicked on a malicious link, El Omari was in truth taken to a website rigged to steal El Omari's email login and password credentials. This password stealing website, "internetsecuritystandards.site," was created on the same date as the email of January 12, 2017, and was deleted a month later on

February 19, 2017. On or about January 12, 2017, El Omari's above email account was accessed without his authorization using his stolen login credentials by CyberRoot logging into El Omari's online Microsoft Outlook email account, ceo@oussamaelomari.com, which uses a Microsoft data center containing physical computer devices for the processing and storing of data. Confidential and privileged email communications between El Omari and his undersigned attorney were then copied and disseminated. In January 2023, one copy was discovered on Del Rosso's Laptop.

50) The Laptop of Dechert LLP's investigator, Del Rosso, discovered in January 2023 has caused new and ongoing injury to El Omari beginning in January 2023. To date, El Omari's damages are in excess of tens of thousands of dollars paid to date in legal fees and costs, and forensic computer investigation costs related to investigating, assessing the scope of the hacking, and seeking to restore the complete loss of the confidentiality of the emails.

51) El Omari sustained injuries to his business and property by reason of the Defendants' actions. The damage to El Omari, proximately caused by the violations, were pecuniary injuries to a proprietary interest. But for the Defendants' violations involving the hacking of El Omari's email account, El Omari would not have had to suffer monetary expenses in spending tens of thousands of dollars from January 2023 to date of investigating the hacking and for attorney fees and costs seeking to assess the hacking and seeking to restore the complete loss of the confidentiality of the emails.

52) Compensation is sought for the value of the loss of confidentiality of the data in each attorney-client communication email. El Omari suffered the complete loss of the valuable confidentiality of the data in the attorney-client communication emails which relate to El Omari's NY litigation. This illegally obtained intelligence included confidential information

about matters and decisions related to investigations, witnesses, legal strategy, evidence, and funding, all of which El Omari takes an active and involved interest. The information had value not only because of the cost of legal services to El Omari at the time, but because of the role of the emails and information therein in the operation and decision-making in El Omari's litigation. El Omari completely lost the confidentiality of his litigation emails and this action seeks to restore the confidentiality of the emails. The loss of the confidentiality of his litigation emails is a recoverable damage under 18 U.S.C. § 1030(e)(8) as an impairment to the integrity of the information. Attorney fees and costs in this action are recoverable losses under 18 U.S.C. § 1030(e)(11) as a cost of responding to an offense and restoring the information to its condition prior to the offense.

53) Punitive damages are sought as an enhancement of compensatory damages because of the wanton, reckless, malicious, and oppressive character of the acts complained of. The Defendants hired and paid CyberRoot, a known mercenary cyber hacker, to gain sensitive and confidential intelligence about their adversary, El Omari. The hacking cost of \$577,049.04 in dozens of small wire transfer amounts during the time period is substantial for a private investigator. The specialized knowledge and duties imposed upon the Defendants by the NYSBA Rules of Professional Conduct, including Rule 1.6 (Confidentiality of Information), shows knowledge of their wrongful conduct and an intention to cover up and hide the Defendants' willful, reckless, and wanton disregard for the confidentiality rights of their hacking target, El Omari, justifying punitive damages against the Defendants.

54) This civil cause of action for compensatory damages and equitable and injunctive relief is authorized under 18 U.S.C. § 1030(g) and § (c)(4)(A)(i)(I). Since January 2023, the

economic loss to El Omari are damages within a 1-year period in excess of \$5,000 expended in forensic computer investigation costs and attorney fees in this proceeding.

55) All in violation of Title 18, United States Code, Sections 1030(a)(2)(C)

SECOND CAUSE OF ACTION

(18. U.S.C. § 1030(b) - Conspiracy to Commit an Offense under 18 U.S.C. § 1030(a))

56) Paragraphs 16 through 56 are realleged and incorporated as if fully set forth herein.

57) Beginning at a time unknown, but no later than July 28, 2015 when Del Rosso sent the first hacking payment to CyberRoot, and continuing to at least on or about January 12, 2017 when El Omari's instant email account was accessed without authorization, the Defendants,

Dechert LLP, and
Nicholas Del Rosso,

did knowingly conspire and agree with each other to commit an offense under 18 U.S.C. § 1030(a)(2)(C), that is, to access the email accounts of El Omari, without authorization, and for purposes of gaining information from El Omari.

Manner and Means of the Conspiracy

58) The object of the conspiracy was to obtain information that would assist the client of Del Rosso, Dechert LLP, in the client's civil lawsuits in New York and elsewhere. Gerrard hired Del Rosso on behalf of Dechert LLP and Del Rosso was paid by Dechert LLP. Del Rosso hired CyberRoot to hack into the email accounts of El Omari, and others, with the information obtained to be shared with Dechert NY for use in the NY litigation.

59) It was part of the conspiracy that, to access El Omari's email accounts without authorization, Del Rosso hired CyberRoot by paying CyberRoot over \$500,000 between July 2015 and December 2016 to send phishing and malicious emails to El Omari using false

identities in order to trick El Omari into opening an attachment and clicking a link in the attachment, which in truth would take El Omari to a credential stealing website. The then stolen username and password credentials would be used to gain unauthorized access to El Omari's email accounts, and to copy El Omari's confidential legal correspondence emails.

60) It was part of the conspiracy that phishing emails were sent to El Omari on the following dates, and possibly other dates.

Date	Account Type	Account Holder
12/20/2016	Gmail Email Account, abousami2793@gmail.com	Oussama El Omari
01/03/2017	Microsoft Outlook Email Account, ceo@oussamaelomari.com	Oussama El Omari
01/12/2017	Gmail and Microsoft Email Accounts, ceo@oussamaelomari.com abousami2793@gmail.com	Oussama El Omari

61) It was further part of the conspiracy that Del Rosso would store El Omari's stolen emails on his devices.

62) The Laptop of Dechert LLP's investigator, Del Rosso, discovered in January 2023 has caused new and ongoing injury to El Omari beginning in January 2023. To date, El Omari's damages are in excess of tens of thousands of dollars paid to date in legal fees and costs, and forensic computer investigation costs related to investigating and seeking to remedy the complete loss of the confidentiality of the emails.

63) El Omari sustained injuries to his business and property by reason of the Defendants' actions. The damage to El Omari, proximately caused by the violations, were pecuniary injuries to a proprietary interest. But for the Defendants' violations involving the hacking of El Omari's email account, El Omari would not have had to suffer monetary expenses of investigating the hacking and spending attorney fees and costs seeking to remedy the complete loss of the confidentiality of the emails.

64) Compensation is sought for the value of the loss of confidentiality of the data in each attorney-client communication email pertaining to the NY litigation. El Omari suffered a complete loss of valuable confidentiality of the data in the attorney-client communication emails pertaining to El Omari's NY litigation. This illegally obtained intelligence would include confidential information about matters and decisions related to investigations, witnesses, legal strategy, evidence, and funding, all of which El Omari takes an active and involved interest. The information had value not only because of the cost of legal services to El Omari at the time, but because of the role of the emails and information therein in the operation and decision-making in El Omari's litigation. El Omari completely lost the confidentiality of his litigation emails and this action seeks to restore the confidentiality of the emails. The loss of the confidentiality of El Omari's litigation emails is sought as a recoverable damage under 18 U.S.C. § 1030(e)(8) as an impairment to the integrity of the information. Attorney fees and costs in this action are recoverable losses under 18 U.S.C. § 1030(e)(11) as a cost of responding to an offense and restoring the information to its condition prior to the offense.

65) Punitive damages are sought as an enhancement of compensatory damages because of the wanton, reckless, malicious, and oppressive character of the acts complained of. The Defendants hired and paid CyberRoot, a known mercenary cyber hacker, to gain sensitive

and confidential intelligence about their adversary, El Omari. The hacking cost of \$577,049.04 in dozens of small wire transfer amounts during the time period is substantial for a private investigator. The specialized knowledge and duties imposed upon the Defendants by the NYSBA Rules of Professional Conduct, including Rule 1.6 (Confidentiality of Information), shows knowledge of their wrongful conduct and an intention to cover up and hide the Defendants' willful, reckless, and wanton disregard for the confidentiality rights of their hacking target, El Omari, justifying punitive damages against the Defendants.

66) This civil cause of action for compensatory damages, and equitable and injunctive relief is authorized under 18 U.S.C. § 1030(g) and § (c)(4)(A)(i)(I). Since January 2023, the economic loss to El Omari are damages to date, and within a 1-year period, in excess of \$5,000 expended in forensic computer investigation costs and attorney fees in this proceeding to investigating the hacked email evidence discovered on Del Rosso's Laptop in January 2023, and seeking relief in this case.

67) All in violation of Title 18, United States Code, Sections 1030(b).

THIRD CAUSE OF ACTION
(Conversion under the Common Law of North Carolina)

68) The factual allegations in paragraphs 16 through 46 are realleged and incorporated as if fully set forth herein.

69) On or about the date set forth below,

Dechert LLP, and
Nicholas Del Rosso,

themselves and through their employees and agents, converted confidential emails of El Omari. Until the time said Defendants accessed and came into possession of each and every email of El Omari found on Del Rosso's Laptop, El Omari was the lawful owner and was entitled to

immediate possession. The Defendants converted each and every such email to their own use by the unauthorized exercise of ownership over each email, depriving El Omari of his right to dominion and control over each and every email, and depriving El Omari of the confidentiality of each such email.

Date	Account Type	Account Holder
01/12/2017	Microsoft Outlook Email Account, ceo@oussamaelomari.com	Oussama El Omari

70) The Laptop of Dechert LLP's investigator, Del Rosso, discovered in January 2023 has caused new and ongoing injury to El Omari beginning in January 2023. To date, El Omari's damages are in excess of tens of thousands of dollars paid to date in legal fees and costs, and forensic computer investigation costs related to investigating and seeking to remedy the complete loss of the confidentiality of the emails.

71) El Omari sustained injuries to his business and property by reason of the Defendants' actions. The damage to El Omari, proximately caused by the violations, were pecuniary injuries to a proprietary interest. But for the Defendants' violations involving the hacking of El Omari's email account, El Omari would not have had to suffer monetary expenses of investigating the hacking and spending attorney fees and costs seeking to remedy the complete loss of the confidentiality of the emails.

72) Compensation is sought for the value of the loss of confidentiality of the data in each attorney-client communication email pertaining to the NY litigation. El Omari suffered the complete loss of valuable confidentiality of the data in the attorney-client communication emails pertaining to El Omari's NY litigation. This illegally obtained intelligence would include

confidential information about matters and decisions related to investigations, witnesses, legal strategy, evidence, and funding, all of which El Omari takes an active and involved interest. The information had value not only because of the cost of legal services to El Omari at the time, but because of the role of the emails and information therein in the operation and decision-making in El Omari's litigation.

73) Punitive damages under North Carolina General Statutes Chapter 1D are sought as an enhancement of compensatory damages because of the wanton, reckless, malicious, and oppressive character of the acts complained of. The Defendants' acts of employing hacking to illegally obtain an adversary's confidential legal communications to assist in litigation, and the Defendants' hiring of CyberRoot, a known mercenary cyber hacker, and in addition, the payment of over one-half million dollars sent in dozens of small wire transfer amounts during the time period, shows an intention to coverup the Defendants' willful, reckless, and wanton disregard for the confidentiality rights of their adversary and hacking target, El Omari, justifying punitive damages against the Defendants.

74) Equitable and injunctive relief is sought pursuant to Fed. R. Civ. P. 65.

75) All under the laws of North Carolina and Fed. R. Civ. P. 65.

WHEREFORE, Plaintiff hereby demands judgment:

A. Preliminarily and permanently enjoining Defendants from taking any action to erase, destroy, or manipulate any evidence of the activities described in this Complaint, or from directing or permitting any third-party from taking any such action; and

B. Preliminarily and permanently enjoining Defendants from using in any way the information obtained from Plaintiff as a result of the alleged wrongdoing; and

C. Permanently enjoining the Defendants from soliciting any third party to access or attempt to access any electronic communications made by Plaintiff and not directed to Defendants, if such action would violate any state or federal statutory or common law; and

D. Ordering that, after issuance of a final, non-appealable judgment in this action and then only with the express permission of this Court of Plaintiff, Defendants to destroy all the information obtained from Plaintiff as a result of the alleged wrongdoing in their possession, custody or control; and

E. Awarding damages in an amount to be determined at trial, including attorneys' fees and costs, punitive damages; and

F. Awarding any such other, further and different relief as the Court shall deem proper.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: New York, New York
June 1, 2023

MOORE INTERNATIONAL LAW PLLC.

/s/ Scott M. Moore

By: _____
Scott Michael Moore, Esq.
Attorneys for Plaintiff, Oussama El Omari
45 Rockefeller Plaza, 20th Floor
New York, New York 10111
T. (212) 332-3474
F. (212) 332-3475
E. mmm@milopc.com